UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/316,804	05/21/1999	JOHN RAITHEL HIND	CR9-99-045	8334

25259 7590 12/10/2003

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2131	7

DATE MAILED: 12/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PR4

Office Action Summary	Application No. 09/316,804	Applicant(s) HIND ET AL.	
	Examiner Ronald Baum	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 November 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-9,11-15 and 17-22* is/are rejected.

7)☒ Claim(s) *4,10 and 16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 30 November 2003.

2. Claims 1-22 are pending for examination.

3. Claims 1-3,5-9,11-15,17-22 are rejected.

Specification

4. The disclosure objections relating to missing application numbers is withdrawn.

Claim Objections

5. The claim objections relating to minor typographical errors, etc., is withdrawn.

Claim Rejections - 35 USC § 101

6. The claim rejections relating to non-statutory subject matter as they either recite a computer comprising instructions or are disclosed as software alone is withdrawn.

Claim Rejections - 35 USC § 112

7. The claim rejections relating to insufficient antecedent basis is withdrawn.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1- 3, 5- 9, 11-15, 17- 22 remain rejected under 35 U.S.C. 102(b) as being anticipated by Debry, U.S. Patent 6,314,521 B1.

8. As per claim 1 ; " A method for *initializing* [see Debry, col. 6, lines 4-7] a first device distributed with an embedded radio module using a server, said server having an *embedded radio* [col. 6, lines 16-17, col. 7, lines 20-24] module, said method comprising the steps of: sending an *inquiry* [col. 6, lines 33-35, the inquiry as part of the establishment of the HTTP session (i.e., SSL mutual authentication handshaking)], where from said server to said first device using said embedded radio modules; *returning* [col. 6, lines 36-43], from said first device, a *unique device identifier* [col. 6, lines 19-27,40-41, col. 8, lines 17-25] of said first device, to said server; creating, at said server, a *public key, private key pair* [col. 6, lines 56-60] for said first device; creating, at said server, a *device certificate* [col. 6, lines 12-18, col. 9, lines 15-23] for said first device, said device certificate having a unique hardware identifier associated with said first device and a public key associated with said first device; *transmitting* [col. 6, lines 52-64] said private key, and said *device certificate* [col. 7, lines 25-26], and a public key of a *Certificate Authority* [col. 6, lines 10-11, col. 8, lines 26-28, 38-44] which signed said device certificate, to said first device; and, storing said private key in *non-removable protected storage* [col. 6, lines 28-32, 66-67] at said first device." ;

And further as per claim 7 ; "A system [This claim is the apparatus of the method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above] for initializing a first device distributed with an embedded radio module using a server, said server having an

embedded radio module, said system comprising: a communications mechanism for sending an inquiry from said server to said first device using said embedded radio modules, and returning, from said first device, a unique device identifier of said first device, to said server; a processor at said server for creating a public key, private key pair for said first device; a device certificate, created at said server, for said first device, said device certificate having a unique hardware identifier associated with said first device and a public key associated with said first device; wherein said communications mechanism transmits said private key, and said device certificate, and a public key of a Certificate Authority which signed said device certificate, to said first device; and, said processor stores said private key in non-removable protected storage at said first device.";

And further as per claim 13 ; "A computer program product embodied in a machine readable medium [This claim is the software embodiment of the method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above] for initializing a first device distributed with an embedded radio module using a server, said server having an embedded radio module, wherein said computer program product comprises the programming steps of: sending an inquiry from said server to said first device using said embedded radio modules; returning, from said first device, a unique device identifier of said first device, to said server; creating, at said server, a public key, private key pair for said first device; creating, at said server, a device certificate for said first device, said device certificate having a unique hardware identifier associated with said first device and a public key associated with said first device; transmitting said private key, and said device certificate, and a public key of a Certificate Authority which

signed said device certificate, to said first device; and, storing said private key in non-removable protected storage at said first device. " ;

9. As per claim 5 ; "A method for *initializing* [see Debry, col. 6, lines 4-7] a first device distributed with an *embedded radio* [col. 6, lines 16-17, col. 7, lines 20-24] module using a server, said server having an embedded radio module, said method comprising the steps of: sending an *inquiry* [col. 6, lines 33-35, the inquiry as part of the establishment of the HTTP session (i.e., SSL mutual authentication handshaking)] from said server to said first device using said embedded radio modules; *creating* [col. 6, lines 19-27,40-41, col. 8, lines 17-25], at said first device, a public key, private key pair for said first device; *storing* [col. 6, lines 28-32, 66-67], at said first device, said private key in non-removable protected storage; *returning* [col. 6, lines 36-43], from said first device, a unique device identifier and said public key of said first device, to said server; creating, at said server, a *device certificate* [col. 6, lines 12-18, col. 9, lines 15-23]for said first device, said device certificate having said device identifier and said public key; and *transmitting* [col. 6, lines 52-64] said device certificate and a public key of a *Certificate Authority* [col. 6, lines 10-11, col. 8, lines 26-28, 38-44] which signed said device certificate to said first device." [col. 10, lines 1-60, figure 11, '...the other configuration data determines which request headers will be passed to the Transaction Gateway Client. Some options include *authentication data*, URI, document root, and Web Browser IP address ... '];

And further as per claim 11 ; "An initialization system [This claim is the apparatus of the method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above], said system comprising: a first device, said first device having an embedded radio module; a server, said server having an embedded radio module; a communications mechanism, said

communications mechanism sending an inquiry from said server to said first device using said embedded radio modules; wherein said first device creates a public key, private key pair for said first device, stores said private key in non-removable protected storage, and returns a unique device identifier and said public key of said first device, to said server; said server creates a device certificate for said first device, said device certificate having said device identifier and said public key; and transmits said device certificate and a public key of a Certificate Authority which signed said device certificate to said first device.";

And further as per claim 17 ; "A computer program product embodied in a machine readable medium [This claim is the software embodiment of the method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above] for initializing a first device distributed with an embedded radio module using a server, said server having an embedded radio module, wherein said computer program product comprises the programming steps of: sending an inquiry from said server to said first device using said embedded radio modules; creating, at said first device, a public key, private key pair for said first device; storing, at said first device, said private key in non-removable protected storage; returning, from said first device, a unique device identifier and said public key of said first device, to said server; creating, at said server, a device certificate for said first device, said device certificate having said device identifier and said public key; and transmitting said device certificate and a public key of a Certificate Authority which signed said device certificate to said first device.";

10. Claim 2 ***additionally recites*** the limitations that "... said protected storage is *write-only storage* able to perform computations involving previously written data. ". The teachings of Debry (col. 6, lines 66-67) suggest such limitations (i.e., non-volatile memory);

And further, claim 8 ***additionally recites*** the limitations that "... wherein said protected storage is write-only storage able to perform computations involving previously written data. " [This claim is the apparatus of the method claim 2, and is rejected for the same reasons provided for the claim 2 rejection above] ;

And further, claim 14 ***additionally recites*** the limitations that "...wherein said protected storage is write-only storage able to perform computations involving previously written data. " [This claim is the software embodiment of the method claim 2, and is rejected for the same reasons provided for the claim 2 rejection above];

11. Claim 3 ***additionally recites*** the limitations that "... wherein a copy of said certificate is stored in an *enterprise database.*". The teachings of Debry (col. 6, lines 24-26, 61-64) suggest such limitations (i.e., IBM Corp. wide database is clearly an enterprise database);

And further, claim 9 ***additionally recites*** the limitations that "... wherein a copy of said certificate is stored in an enterprise database. " [This claim is the apparatus of the method claim 3, and is rejected for the same reasons provided for the claim 3 rejection above];

And further, claim 15 ***additionally recites*** the limitations that "... wherein a copy of said certificate is stored in an enterprise database. " [This claim is the software embodiment of the method claim 3, and is rejected for the same reasons provided for the claim 3 rejection above];

12. Claim 19 ***additionally recites*** the limitations that "... wherein communications between said first device and said server is performed in a wireless manner."; The teachings of Debry (col. 6, lines 16-17, col. 7, lines 20-24) suggest such limitations;

And further, claim 20 ***additionally recites*** the limitations that "... wherein communications between said first device and said server is performed in a wireless manner."

[This claim is the apparatus of the method claim 19, and is rejected for the same reasons provided for the claim 19 rejection above];

And further, claim 21 ***additionally recites*** the limitations that "... wherein communications between said first device and said server is performed in a wireless manner." [This claim is the software embodiment of the method claim 19, and is rejected for the same reasons provided for the claim 19 rejection above];

And further, claim 22 ***additionally recites*** the limitations that "... wherein communications between said first device and said server is performed in a wireless manner." The teachings of Debry (col. 6, lines 16-17, col. 7, lines 20-24) suggest such limitations;

13. Claim 6 ***additionally recites*** the limitations that "... wherein said protected storage is a write-only storage able to perform computations involving previously written data." . The teachings of Debry (col. 6, lines 66-67) suggest such limitations (i.e., non-volatile memory);

And further, claim 12 ***additionally recites*** the limitations that "... wherein said protected storage is a write-only storage able to perform computations involving previously written data." [This claim is the apparatus of the method claim 6, and is rejected for the same reasons provided for the claim 6 rejection above];

And further, claim 18 ***additionally recites*** the limitations that "... wherein said protected storage is a write-only storage able to perform computations involving previously written data." [This claim is the software embodiment of the method claim 6, and is rejected for the same reasons provided for the claim 6 rejection above];

Allowable Subject Matter

14. Claims 4,10,16 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

15. As per applicant's argument concerning the Debry reference teachings not suggesting the use of wireless communications technique, the examiner directs the applicant's attention to col. 6,lines 16-17, and col. 7,lines 20-24, whereas it is inherent that the cell phone (and inherent accompanying base station component) clearly is a wireless communications technology in a client server architecture environment. Therefore, the examiner finds the applicants arguments not to be persuasive.

16. As per applicant's argument concerning the Debry reference teachings not suggesting the use of wireless communications technique in a inquiry of the client by the server, the examiner directs the applicant's attention to col. 6,lines 33-34, whereas it is inherent that the HTTP session establishment protocol is bi-directional (i.e., SSL cryptographic parameter/key setup during secure communications setup). Therefore, while the applicant's arguments have been fully considered, they are not persuasive.

17. As per applicant's argument concerning the Debry reference teachings not suggesting the use of private keys, and said key storage in non-removable memory at the client, the examiner disagrees in that at the very least, digital certificates are a function of a public and private key in

order to effect the authentication cryptographic function. Therefore, while the applicants arguments have been fully considered, they are not persuasive.

18. As per applicant's argument concerning the Debry reference teachings not suggesting the use of private and public keys, and said keys generated at the client, the examiner disagrees. Therefore, while the applicant's arguments have been fully considered, they are not persuasive.

19. As per applicant's argument concerning the Debry reference teachings not suggesting the creating at the server, and forwarding to the client, a client unique (digital) certificate (and associate keys a function of the client ID), the examiner disagrees. Therefore, while the applicant's arguments have been fully considered, they are not persuasive.

20. As per applicant's argument concerning the Debry reference teachings not suggesting the storage of the client unique (digital) certificate (and associate keys a function of the client ID), on a database of enterprise scope (i.e., at the level of a certificate authority), the examiner disagrees. Therefore, while the applicant's arguments have been fully considered, they are not persuasive.

21. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

22. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100